



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|-----------------|-------------|----------------------|---------------------|------------------|
| 10/612,198      | 07/01/2003  | Carey Nachenberg     | 20423-07775         | 4107             |

34415 7590 01/17/2007  
SYMANTEC/ FENWICK  
SILICON VALLEY CENTER  
801 CALIFORNIA STREET  
MOUNTAIN VIEW, CA 94041

|          |
|----------|
| EXAMINER |
|----------|

L.OVING, JARIC E

|          |              |
|----------|--------------|
| ART UNIT | PAPER NUMBER |
|----------|--------------|

2137

| SHORTENED STATUTORY PERIOD OF RESPONSE | NOTIFICATION DATE | DELIVERY MODE |
|--|-------------------|---------------|
| 3 MONTHS                               | 01/17/2007        | ELECTRONIC    |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Notice of this Office communication was sent electronically on the above-indicated "Notification Date" and has a shortened statutory period for reply of 3 MONTHS from 01/17/2007.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ptoc@fenwick.com  
bhoffman@fenwick.com  
qdinh@fenwick.com

**Office Action Summary**

Application No.

10/612,198

Applicant(s)

NACHENBERG ET AL.

Examiner

Jaric Loving

Art Unit

2137

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 19 October 2006.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1 and 3-21 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1 and 3-21 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 01 July 2003 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO/SB/08)  
Paper No(s)/Mail Date \_\_\_\_\_
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date: \_\_\_\_\_
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: \_\_\_\_\_

## **DETAILED ACTION**

### ***Response to Amendment***

1. This office action is responsive to Applicant's amendment received on October 19, 2006. Claims 1 and 3-21 are pending. Claim 2 has been cancelled. Claim 21 is new.
2. The 35 USC § 112 and double patenting rejections have been withdrawn due to Applicant's amendment.
3. Applicant's arguments filed on October 19, 2006 have been fully considered, but they are not persuasive.

### ***Claim Rejections - 35 USC § 103***

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

2. Claims 1-6, 8-17, 19-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Desai et al., US 2003/0188189 and further in view of Harkins, US 6,775,827.

In claims 1 and 16, Desai discloses a computer implemented method and computer-readable medium containing computer program instructions for training a database intrusion detection system in real time (paragraphs [0035], [0043], [0052], [0056]), but fails to disclose: observing, in real time, commands that are accessing the database; and deriving from said commands, in real time, a set of acceptable

commands. Harkins discloses observing, in real time, commands that are accessing the database (col. 4, lines 13-17); and deriving from said commands, in real time, a set of acceptable commands (col. 5, lines 41-49 – execution profiles contain frequently selected commands, thus they are similar to set of acceptable commands).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine Desai's intrusion detection system with Harkins' real time audit method that observe and derive acceptable commands to effectively examine programs during execution in real time. It is for this reason that one of ordinary skill in the art would have been motivated to provide Desai's intrusion detection system with real time auditing because it provides a quick, comprehensive analysis of a program's execution and also allows identification and resolution of any problems (Harkins, col. 2, lines 10-23).

In claim 3, Desai, as modified, discloses the method of claim 2 wherein the commands are SQL commands (Desai, paragraph [0056]).

In claim 4, Desai, as modified, discloses the method of claim 1 wherein at least one observed command is from the group of commands comprising a query, an add, a delete, and a modify (Desai, paragraphs [0052], [0092] – search of a database is similar to query).

In claims 5 and 17, Desai, as modified, discloses the method and computer-readable medium of claims 1 and 16, respectively, wherein the deriving step comprises: grouping the commands into categories (Desai, paragraphs [0050]-[0052]); and

updating statistical information pertaining to the categories in real time (Desai, paragraph [0062]).

In claim 6, Desai, as modified, discloses the method of claim 5 wherein the categories comprise at least one category from the group of categories comprising:

canonicalized commands;  
dates and times at which commands access the database (Desai, paragraphs [0050]-[0052]);

logins of users that issue commands;  
identities of users that issue commands;  
departments of users that issue commands;  
applications that issue commands;  
IP addresses of issuing users;  
frequency of issuing commands by users;  
identities of users accessing a given field within the database;  
times of day that a given user accesses a given field within the database;  
fields accessed by commands;  
combinations of fields accessed by commands;  
tables within the database accessed by commands;  
combinations of tables within the database accessed by commands.

In claim 8, Desai, as modified, discloses the method of claim 1 wherein the observing step comprises at least one of:

real-time auditing (Harkins, col. 4, lines 13-17); and

in-line interception (Desai, paragraph [0042]).

In claim 9, Desai, as modified, discloses the method of claim 8 wherein the observing step comprises real-time auditing; and at least one of the following is used to extract the commands for observation:

- an API that accesses the database;
- code injection (col. 9, lines 5-28);
- patching;
- direct database integration.

In claim 10, Desai, as modified, discloses the method of claim 8 wherein the observing step comprises in-line interception; and at least one of the following is interposed between senders of the commands and the database:

- a proxy;
- a firewall (Desai, paragraph [0042]);
- a sniffer (Desai, paragraph [0091]);

In claim 11, Desai, as modified, discloses the method of claim 1 wherein:

- during the deriving step, suspicious activity is tracked (Desai, paragraph [0054]);

and

- subsequent to the deriving step, the suspicious activity is reported to a system administrator (Desai, paragraphs [0076]-[0077]).

In claim 12, Desai, as modified, discloses the method of claim 1 wherein a duration of performing the deriving step is determined by statistical means (Desai, paragraph [0062]).

In claims 13 and 19, Desai, as modified, discloses the method and computer-readable medium of claims 1 and 16, respectively, further comprising, subsequent to the deriving step, as operational step in which commands that are accessing the database are compared against the set of acceptable commands (Harkins, col. 2, lines 56-58).

In claim 14, Desai, as modified, discloses the method of claim 13 wherein a command that is accessing the database during the operational step that does not match a command in the set of acceptable commands is flagged as suspicious (Desai, paragraph [0054]).

In claim 15, Desai, as modified, discloses the method of claim 14 wherein, when a command is flagged as suspicious, at least one of the following is performed:

- an alert is sent to a system administrator (Desai, paragraphs [0076]-[0077]);
- the command is not allowed to access the database;
- the command is allowed to access the database, but the access is limited;
- the command is augmented;
- a sender of the command is investigated.

In claim 20, Desai discloses apparatus for training a database intrusion detection system in real time (paragraphs [0035], [0043], [0052], [0056]), but fails to disclose: a training module adapted for observing, in real time, commands that are accessing the database, and for deriving from said commands, in real time, a set of acceptable commands; coupled to the set of acceptable commands, a comparison module for comparing commands that access the database during an operational phase with

commands in the set of acceptable commands. Harkins discloses observing, in real time, commands that are accessing the database (col. 4, lines 13-17), and for deriving from said commands, in real time, a set of acceptable commands (col. 5, lines 41-49 – execution profiles contain frequently selected commands, thus they are similar to set of acceptable commands); coupled to the set of acceptable commands, a comparison module for comparing commands that access the database during an operational phase with commands in the set of acceptable commands (col. 2, lines 56-58).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine Desai's intrusion detection system with Harkins' real time audit method that observe and derive acceptable commands, and compare commands accessing the computer to effectively examine programs during execution in real time. It is for this reason that one of ordinary skill in the art would have been motivated to provide Desai's intrusion detection system with real time auditing because it provides a quick, comprehensive analysis of a program's execution and also allows identification and resolution of any problems (Harkins, col. 2, lines 10-23).

3. Claims 7 and 18 rejected under 35 U.S.C. 103(a) as being unpatentable over Desai and Harkins and further in view of Pandit et al., US 2003/0154402.

In claims 7 and 18, Desai and Harkins disclose the method and computer-readable medium of claims 5 and 17, respectively, but fail to disclose the categories comprise canonicalized commands; and each category is a command stripped of literal field data. Pandit discloses the categories comprise canonicalized commands (paragraph [0037] – placeholders placed in templates); and each category is a

command stripped of literal field data (paragraph [0037] – data values can be entered in place of placeholders).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine Desai's intrusion detection system and Harkins' real time audit method with Pandit's system of storing events utilizing canonicalized commands to serve as placeholders for events. It is for this reason that one of ordinary skill in the art would have been motivated to provide Desai's intrusion detection system and Harkins' real time audit method with canonicalized commands because it helps automate the process of creating a database (Pandit, paragraph [0038]).

4. Claim 21 is rejected under 35 U.S.C. 103(a) as being unpatentable over Desai and further in view of Harkins and Pandit.

In claim 21, Desai discloses a computer-readable medium containing computer program instructions for providing a database intrusion detection system (paragraphs [0035], [0043], [0052], [0056]); grouping the commands (paragraphs [0050]-[0052]) and flagging as suspicious a command that accesses the database during an operation phase (paragraphs [0054], [0076]-[0077]), but fails to disclose observing commands that are accessing a database during a training phase, the commands comprising literal field data; stripping the commands of literal field data to produce commands in canonical forms; grouping the commands responsive to the commands' canonical forms; generating a set of acceptable commands responsive to the grouped commands; comparing commands that access the database during an operation phase with commands in the set of acceptable commands. Harkins discloses observing

Art Unit: 2137

commands that are accessing a database during a training phase, the commands comprising literal field data (col. 4, lines 13-17); generating a set of acceptable commands responsive to the grouped commands (col. 5, lines 41-49); comparing commands that access the database during an operation phase with commands in the set of acceptable commands (col. 2, lines 56-58). Pandit discloses stripping the commands of literal field data to produce commands in canonical forms (paragraph [0037]).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine Desai's intrusion detection system with Harkins' real time audit method that observe and derive acceptable commands, and compare commands accessing the computer to effectively examine programs during execution in real time. It is for this reason that one of ordinary skill in the art would have been motivated to provide Desai's intrusion detection system with real time auditing because it provides a quick, comprehensive analysis of a program's execution and also allows identification and resolution of any problems (Harkins, col. 2, lines 10-23).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine Desai's intrusion detection system and Harkins' real time audit method with Pandit's system of storing events utilizing canonicalized commands to serve as placeholders for events. It is for this reason that one of ordinary skill in the art would have been motivated to provide Desai's intrusion detection system and Harkins' real time audit method with canonicalized commands because it helps automate the process of creating a database (Pandit, paragraph [0038]).

***Response to Arguments***

5. Regarding claims 1 and 3-21, Applicant basically argues the Desai, Harkins, and Pandit references are inapplicable to claims 1-2, 4, 13, 19, 20 and the remaining claims are therefore allowable.

As to claim 1, Applicant argues "... Desai neither discloses nor suggests monitoring for attacks on [the attack signature] database." Examiner contends otherwise. Paragraph [0052] in Desai provides "... the attack signature database contains "known" signatures from prior and previously encountered attacks. If a "match" is found, an alert is generated. This suggests the database is indeed monitored, if a match is to be determined.

Applicant also argues "Paragraph [0056]... provides no teaching or suggestion of how to detect database intrusions based on [SQL traffic] monitoring." Examiner contends otherwise. Paragraph [0056] describes a basis of establishing categories of normal traffic patterns in an enterprise from which abnormal behavior can be observed. Therefore, the SQL traffic monitoring is performed in this manner.

Next, Applicant argues "Harkins does not disclose a database intrusion detection system" and "Harkins does not teach or suggest 'observing... commands that are accessing [a] database.'" Examiner contends that Harkins was cited for its teaching of real-time analysis of an executing program and not a database intrusion detection system. However, the combination is proper since both inventions involve the observation or monitoring of a computer system and troubleshooting.

Next, Applicant argues that “the fact that an execution profile is frequently selected does not imply that any commands in the profile are acceptable.” Examiner contends otherwise. In col. 5, lines 41-49, Harkins further states “[t]he invention allows a selected execution profile to be modified...” Therefore, if the profile can be modified the most acceptable commands are included.

Next, Applicant argues “Harkins neither discloses nor suggests the comparing element recited by the claims.” Examiner contends otherwise. As Applicant has stated from Harkins, the configuration records are compared by showing the differences between two builds. Thus, Harkins provides for comparing commands. It has already been stated above that Desai provides a database detection system.

Next, Applicant argues “there is no reason why a person of ordinary skill in the art would be motivated to combine Desai and Harkins to create a database intrusion detection system.” As stated previously, Examiner contends that Harkins was cited for its teaching of real-time analysis of an executing program and not a database intrusion detection system. However, the combination is proper since both inventions involve the observation or monitoring of a computer system and troubleshooting.

Next, Applicant argues “Pandit does not disclose or suggest stripping literal field data from database access commands as claimed.” Examiner contends otherwise. In paragraph [0037], Pandit describes a basis for which data values can be entered in place of placeholders. Therefore, the data values in place of placeholders remove literal field data in the database.

Next, Applicant argues that Desai does not disclose that a command is from a group of certain commands. Examiner contends otherwise. Paragraph [0052] describes that a database is searched for a match which is similar to a query. Further, paragraph [0092] describes that the sensor database is regularly updated and this suggests signatures are added or deleted. Examiner also notes that the claim merely requires only at least one of the commands.

***Conclusion***

6. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jaric Loving whose telephone number is (571) 272-1686. The examiner can normally be reached on Monday-Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone

Art Unit: 2137

number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

27

JL

  
EMMANUEL L. MOISE  
SUPERVISORY PATENT EXAMINER